PRIVACY POLICY · HEALTHCARE & CARE DEPLOYMENTS

Data Privacy & Pilot Data Policy

How Venture Robot Solutions handles data during robot pilots and deployments in hospitals and care institutions. What is collected, what is never collected, where it lives, who can access it, and for how long.

EFFECTIVE DATE	COMPANY
22 May 2026	**Venture Robot Solutions, CH**
PRIMARY CLOUD	PRIVACY CONTACT
European infrastructure (Scaleway, FR)	**contact@venturerobotsolutions.com**

PURPOSE

To make robot deployments measurable and safe, without turning robots into surveillance devices.

01 Purpose of this policy

Venture Robot Solutions designs, deploys and operates service robots for hospitals and care institutions. This policy explains how VRS handles data during robot pilots and deployments: what is collected, what is never collected, where data is stored, who can access it, how long it is retained, and how privacy is protected by design. It is intended for pilot partners, healthcare institutions, academic partners and internal VRS stakeholders.

02 Applicable law

- For Swiss-based pilots and deployments, the **Swiss Federal Act on Data Protection (FADP)** applies as the primary data protection law. The FADP protects the personality and fundamental rights of natural persons whose personal data is processed.
- For pilots or deployments in EU member states, the **GDPR** applies.
- Where both Swiss FADP and GDPR may apply, VRS will apply the stricter operational requirement where reasonably possible.

03 Our role: controller or processor

In most healthcare and care pilots, the partner institution is expected to act as the **data controller** for pilot-related data collected in its environment, and VRS is expected to act as **data processor** under the partner institution's instructions. VRS may act as data controller for its own website, sales, support, internal operations, product improvement, anonymised research outputs and internal technical analytics. The exact controller / processor role will be defined in the pilot agreement, data processing agreement or collaboration agreement with each partner institution.

04 Privacy-by-design principles

VRS follows an **edge-first, data-minimisation approach**. The hard rules below are core product constraints, not optional settings.

Hard rules

- The robot does **not send raw RGB camera footage to the cloud**.
- The robot does **not permanently store raw audio recordings**. Raw audio may be transmitted for transient speech processing where enabled, but is not retained in persistent storage and recordings are not kept.
- The robot does not store patient names, health records, dates of birth or medical files.
- The robot does not perform facial recognition, voice identification or biometric identification.
- The robot does not monitor individual staff performance.

Raw RGB camera footage is processed locally on the robot and is not sent to the cloud. **Depth images and other onboard sensor data may be collected and stored.** Microphone signals may be transmitted for transient speech processing where enabled, via the **Mistral AI API** (European hosting), but raw audio is not retained. Derived operational signals are sent to the cloud, such as robot position, mission status, anonymous obstacle detections, interaction timestamps and system health.

05 Workplace and staff privacy

VRS robots are not designed to monitor staff behaviour or individual work performance. The purpose of data collection is to evaluate robot safety, mission execution, workflow fit, operational usefulness and human-robot interaction quality. The FDPIC states that video surveillance systems may only be used in the workplace when less invasive measures are unsuitable, and workers should not be filmed except in exceptional cases. **VRS will not use pilot data to rank, score or evaluate individual staff members.**

06 Data we collect during pilots and deployments

Robot operational data

- robot ID; site or hospital ID; timestamp; current map ID;
- robot position and motion; mission state; battery and charging status;
- mission start and end; mission outcome; distance travelled; failure reason;
- anonymous obstacle or dynamic-map detections; touch-screen interaction events; robot speech events;
- voice activity timestamps without audio content;
- **depth images;**
- **other onboard sensor data** (LiDAR, IMU, odometry, proximity sensors, environmental sensors), excluding raw RGB camera footage;
- coarse intent labels, where enabled.

Pilot evaluation data

- anonymised feedback forms; role-level feedback (nurse, care assistant, ward manager, patient);
- qualitative comments; pilot observer notes; mission KPIs; manually labelled pilot events;
- anonymised datasets for research or evaluation.

Dashboard and account data

- email address; role and access rights; authentication data;
- audit logs; support requests; dashboard activity necessary for security and operation.

07 Data we do not collect

VRS does not collect or transmit to the cloud:

- raw RGB video;
- **persistent storage of raw audio recordings** (raw audio may transit through speech-processing services where enabled, but is not retained);
- patient medical records; patient names or dates of birth;
- facial recognition templates; voice prints; biometric identifiers;
- advertising profiles; marketing tracking cookies; individual staff performance monitoring data.

VRS does not sell personal data.

08 Where data is stored

VRS uses **European cloud infrastructure, currently Scaleway in the Paris region, France**, for database, object storage, compute and IoT communication. Data is not intentionally transferred outside Switzerland or the European Economic Area unless explicitly agreed with the partner institution and legally documented. The robot itself may temporarily store operational data locally, for example during connectivity interruptions. This local buffer is cleared once the data has been transmitted or is no longer necessary.

09 Cloud and sub-processors

Current or potential sub-processors may include:

- Scaleway SAS (Paris, France) for hosting, database, object storage, compute and IoT infrastructure;
- **Mistral AI** (Paris, France; API servers in the EU) for transient speech processing of raw audio where the feature is enabled;
- research partners under NDA and data-sharing agreements;
- healthcare or care partners involved in the pilot.

For external research collaboration, VRS will share only anonymised or pseudonymised datasets where possible. Raw RGB footage, raw audio and direct patient identifiers are not shared. If additional sub-processors are introduced, they will be listed in the relevant pilot agreement, DPA or sub-processor list.

10 Purposes of processing

VRS processes data only for defined purposes: operating robot missions; ensuring safety and reliability; debugging and maintenance; generating pilot KPIs; measuring acceptance and workflow fit; improving CARE-OS and robot behaviour; providing dashboard access; fulfilling contractual obligations; supporting anonymised research and pilot evaluation. VRS does not process pilot data for unrelated advertising, staff surveillance or profiling purposes.

11 Legal bases

Depending on the context, processing may be based on contract; documented instructions from the healthcare or care partner; legitimate interest in operating and improving a deployed system; consent where required; legal obligations; or anonymised research or evaluation purposes where no individual is identifiable. For Swiss-based pilots, the legal basis and responsibility split will be confirmed with the partner institution before deployment.

12 Data Protection Impact Assessment

Before each hospital or care pilot, VRS will support the partner institution in completing a **DPIA** where required or appropriate. The DPIA may cover:

- description of processing; categories of data; data flows;
- risks for staff, patients, residents and visitors; safeguards;
- retention rules; access controls;
- controller / processor responsibilities; sub-processors;
- deletion and anonymisation procedures.

Under Swiss law, a DPIA is required when a planned processing activity may result in a high risk for the personality or fundamental rights of data subjects.

13 Research and pilot data

For research projects, such as collaboration with ZHAW, BFH or other academic partners:

- an NDA and data-sharing agreement should be signed before any data exchange;
- shared datasets should be anonymised or pseudonymised;
- no raw RGB footage should be shared; no raw audio should be shared;
- direct identifiers should be removed; access should be read-only where possible;
- publication should be limited to aggregate findings unless otherwise agreed.

For challenge, thesis or research projects, VRS may provide sandbox datasets, simulated data, anonymised telemetry or read-only database access.

14 Retention

DATA CATEGORY	DEFAULT RETENTION	NOTES
Raw edge buffer	**Until transmitted**	Deleted after transmission or when no longer necessary
Web server logs	**30 days**	Security and abuse prevention
Support records	**Up to 36 months**	After case closure
Live telemetry	**Contract term + 12 mo**	Operational analytics
Mission & fleet analytics	**Contract term + 12 mo**	Operational analytics
Audit logs	**Min. 24 months**	Where required for security
Pilot datasets	**Project + agreed period**	Per research agreement
Anonymised research	**May be retained longer**	If no person can be identified

After the retention period expires, data is deleted or irreversibly anonymised. If a partner institution requires shorter retention periods, these can be defined in the pilot agreement.

15 Machine learning models and derived outputs

Some VRS systems may use pilot data or anonymised operational data to improve future robot behaviour, analytics or evaluation tools. Models trained on pilot data are considered derived outputs. If a partner institution requests deletion of pilot data, VRS will delete or anonymise the source data and assess whether model retraining, model deletion or exclusion of affected sessions from future training is technically feasible and proportionate. **VRS will not train models on raw RGB camera footage, because it is not sent to the cloud, nor on raw audio recordings, because raw audio is not retained in persistent storage.**

16 Security measures

VRS applies technical and organisational security measures, including:

- edge-first processing; TLS for communications; mutual TLS for robot-to-cloud where applicable;
- per-robot certificates or credentials; role-based access control; tenant-level data separation;
- audit logs for sensitive actions; password hashing; optional two-factor authentication;
- encrypted storage where available; limited access to pilot datasets;
- secrets excluded from source code; local buffering during outages;
- deletion or anonymisation after retention expires.

17 Data subject rights

Depending on applicable law and context, individuals may have rights to access their data; request correction; request deletion; restrict processing; object to processing; withdraw consent where consent is the basis; receive a copy of their data where applicable; and lodge a complaint with the competent supervisory authority. In hospital and care deployments, staff, patients or residents should normally contact the healthcare institution first. The institution can then coordinate with VRS where VRS acts as processor.

18 Breach notification

If a data security incident creates a likely risk to affected individuals, VRS will notify the relevant partner institution and cooperate with required notifications. Where VRS acts as processor, VRS will notify the controller without undue delay. Where VRS acts as controller, VRS will follow applicable legal notification obligations under Swiss FADP or GDPR.

19 Children and vulnerable persons

VRS robots may operate in environments where children, elderly persons or vulnerable patients are present. The robot is not designed to identify them. The same privacy-by-design rules apply: no raw RGB cloud upload; **no persistent storage of raw audio;** no identity record; no biometric recognition; no medical decision-making. Additional consent, information or supervision requirements may apply depending on the pilot site.

20 Cookies and website data

VRS does not use advertising cookies or third-party profiling cookies. For its website and dashboard, VRS may use strictly necessary cookies for authentication, security and session management. Standard web server logs may include IP address, user-agent, request path and timestamp and are retained for security and abuse prevention.

21 Changes to this policy

VRS may update this policy as its product, deployments and legal requirements evolve. Material changes will be communicated to relevant partners before they apply to ongoing pilots or deployments. The effective date at the top of the policy always reflects the latest version.

22 · CONTACT

Privacy questions or requests.

EMAIL
contact@venturerobotsolutions.com

COMPANY
Venture Robot Solutions, Switzerland